

On the Courtade-Kumar conjecture for certain classes of Boolean functions

Septimia Sarbu, septimia.sarbu@gmail.com

Abstract—We prove the Courtade-Kumar conjecture, for certain classes of n -dimensional Boolean functions, $\forall n \geq 2$ and for all values of the error probability of the binary symmetric channel, $\forall 0 \leq p \leq \frac{1}{2}$. Let $\mathbf{X} = [X_1 \dots X_n]$ be a vector of independent and identically distributed Bernoulli($\frac{1}{2}$) random variables, which are the input to a memoryless binary symmetric channel, with the error probability in the interval $0 \leq p \leq \frac{1}{2}$, and $\mathbf{Y} = [Y_1 \dots Y_n]$ the corresponding output. Let $f : \{0, 1\}^n \rightarrow \{0, 1\}$ be an n -dimensional Boolean function. Then, the Courtade-Kumar conjecture states that the mutual information $\text{MI}(f(\mathbf{X}), \mathbf{Y}) \leq 1 - H(p)$, where $H(p)$ is the binary entropy function.

Index Terms—Boolean function, mutual information, Karamata's theorem, binary entropy function

I. INTRODUCTION

A recent information-theoretic conjecture, termed the Courtade-Kumar conjecture, was stated in [1] and gives the upper bound on the mutual information between a Boolean function of a random vector of inputs to a memoryless binary symmetric channel and the vector of the outputs. The mutual information is computed between a Boolean function of n independent and identically distributed Bernoulli random variables, with success probability, $q = \frac{1}{2}$, and the output of a memoryless binary symmetric channel, with error probability, $0 \leq p \leq \frac{1}{2}$, when this vector of Bernoulli random variables is passed as its input. The conjecture states that this upper bound is equal to $1 - H(p)$, where $H(p)$ denotes the binary entropy function. Several proofs have appeared in the literature, for different settings of this conjecture, but the most general case has remained unsolved. We bring further contributions to this effort. Using Karamata's theorem [2], we prove the Courtade-Kumar conjecture [1], for certain classes of Boolean functions, $\forall n \geq 2$ and $\forall 0 \leq p \leq \frac{1}{2}$. These functions represent particular subclasses of lex functions, as introduced by Kumar and Courtade in [3]. In the context of this conjecture, Karamata's theorem has been used in an earlier version of the preprint [4], which extends the conjecture to the continuous case. The generalization of Karamata's theorem, named Schur convexity, has been employed in [3].

Our paper is structured as follows: we start the introductory section with the prior results obtained so far in the literature, in the effort to solve the Courtade-Kumar conjecture. We end this section with our contributions. The essence of this paper, the proof of the Courtade-Kumar conjecture for particular classes of Boolean functions, for any dimension $n \geq 2$ and any error probability $0 \leq p \leq \frac{1}{2}$, is given in Section II. We present the conclusions of this study in Section III.

A. Prior work related to the Courtade-Kumar conjecture

The proofs that have made the most progress towards solving the Courtade-Kumar conjecture are [5], [6]. The authors of [5] employ Fourier analysis and the hypercontractivity theorem to prove the bound stated in their Theorem 1, in the case of balanced Boolean functions and p in the range $\frac{1}{2} \cdot \left(1 - \frac{1}{\sqrt{3}}\right) \leq p \leq \frac{1}{2}$: $\text{MI}(f(\mathbf{X}), \mathbf{Y}) \leq \frac{\log(e)}{2} \cdot (1 - 2 \cdot p)^2 + 9 \cdot \left(1 - \frac{\log(e)}{2}\right) \cdot (1 - 2 \cdot p)^4$. They show that this new bound performs better than the previously established bound of $(1 - 2 \cdot p)^2$ of [7], in the case of $\frac{1}{3} \leq p \leq \frac{1}{2}$. In Corollary 1, they prove that the Courtade-Kumar conjecture holds for the dictatorship function, as a special case of equiprobable Boolean functions, when $p \rightarrow \frac{1}{2}$. This region is termed the noise interval $p \in [\frac{1}{2} - \frac{1}{\overline{p}_n}, \frac{1}{2}]$, where \overline{p}_n is defined as $\overline{p}_n = \frac{1}{4} \cdot 2^{-n}$. Related to this result, in Theorem 1.15, the author of [6] proves that the Courtade-Kumar conjecture holds for high noise, that is $\text{MI}(f(\mathbf{X}), \mathbf{Y}) \leq 1 - H(p)$ holds for any Boolean function and for any noise $\epsilon \geq 0$, such that $(1 - 2 \cdot \epsilon)^2 \leq \delta \Leftrightarrow \frac{1}{2} - \frac{\sqrt{\delta}}{2} \leq \epsilon \leq \frac{1}{2} + \frac{\sqrt{\delta}}{2}$, where $\delta > 0$ is a constant of small value. The author of [6] provides an improvement of Theorem 1 derived by Wyner and Ziv in [8], known as Mrs. Gerber's Lemma, which was employed in [7], for the proof of Theorem 4. This strengthening of Mrs. Gerber's Lemma is employed in the proof of the Courtade-Kumar conjecture for high noise [6].

An extension of the Courtade-Kumar conjecture to two n -dimensional Boolean functions, is hypothesized to hold in [9], termed Conjecture 3. It states that, for any Boolean functions $f, g : \{0, 1\}^n \rightarrow \{0, 1\}$, the mutual information $\text{MI}(f(\mathbf{X}), g(\mathbf{Y})) \leq 1 - H(p)$. For several specific cases of the joint probability mass function of the binary random variables $f(\mathbf{X})$ and $g(\mathbf{Y})$, the authors analytically prove another conjecture, termed Conjecture 4, which implies Conjecture 3. A similar form of Conjecture 4 of [9] is analytically proved in [10], in a more general context than that of the results of [9]. In section V of [10], the authors prove that the mutual information $\text{MI}(B, \hat{B}) \leq 1 - H(p)$, for Boolean functions, $B = f(\mathbf{X})$ and $\hat{B} = g(\mathbf{Y})$, an estimator of \mathbf{Y} , with fixed mean $\mathbb{E}(B) = \mathbb{E}(\hat{B}) = a$ and $\mathbb{P}(B = \hat{B} = 0) \geq a^2$. Conjecture 3 of [9] is proved to hold in [11]. The Courtade-Kumar conjecture is generalized to continuous random variables in the preprint [4]. The function f takes as input n -dimensional real vectors, when they are correlated Gaussian random vectors and when they are correlated random vectors from the unit sphere. As output, the function produces values from the set $\{0, 1\}$.

B. Our contributions

Theorem 1: Let $\mathbf{X} = [X_1 X_2 \dots X_n]$ be an n -dimensional random vector of independent and identically distributed Bernoulli($\frac{1}{2}$) random variables and $\mathbf{Y} = [Y_1 Y_2 \dots Y_n]$ the result of sending \mathbf{X} through a discrete memoryless binary symmetric channel, without feedback and with the error probability $0 \leq p \leq \frac{1}{2}$. Let $f : \{0, 1\}^n \rightarrow \{0, 1\}$ be an n -dimensional Boolean function, which has any of the following properties: (1) for any $\mathbf{X}^{(i)} \in \{0, 1\}^n$, $f(\mathbf{X}^{(i)}) = 1, f(\mathbf{X}) = 0, \forall \mathbf{X} \in \{0, 1\}^n, \mathbf{X} \neq \mathbf{X}^{(i)}$; (2) for any $\mathbf{X}^{(i)} \in \{0, 1\}^n$, $f(\mathbf{X}^{(i)}) = 0, f(\mathbf{X}) = 1, \forall \mathbf{X} \in \{0, 1\}^n, \mathbf{X} \neq \mathbf{X}^{(i)}$; (3) $\mathbf{X}^{(i)} = [\mathbf{X}_r \mathbf{X}_{n-r}^{(i)}]$, $\forall \mathbf{X}_{n-r}^{(i)} \in \{0, 1\}^{n-r}$, that is $i \in \{1, 2, \dots, 2^{n-r}\}$, $\forall r \in \{1, 2, \dots, n-1\}$, $f(\mathbf{X}^{(i)}) = 1, f(\mathbf{X}) = 0, \forall \mathbf{X} \in \{0, 1\}^n, \mathbf{X} \neq \mathbf{X}^{(i)}$; (4) $\mathbf{X}^{(i)} = [\mathbf{X}_r \mathbf{X}_{n-r}^{(i)}]$, $\forall \mathbf{X}_{n-r}^{(i)} \in \{0, 1\}^{n-r}$, that is $i \in \{1, 2, \dots, 2^{n-r}\}$, $\forall r \in \{1, 2, \dots, n-1\}$ $f(\mathbf{X}^{(i)}) = 0, f(\mathbf{X}) = 1, \forall \mathbf{X} \in \{0, 1\}^n, \mathbf{X} \neq \mathbf{X}^{(i)}$. Let $H(p)$ denote the binary entropy function. Then,

$$\text{MI}(f(\mathbf{X}), \mathbf{Y}) \leq 1 - H(p), \forall n \geq 2, \forall 0 \leq p \leq \frac{1}{2}.$$

II. PROOF OF THE COURTADE-KUMAR CONJECTURE, FOR CERTAIN CLASSES OF n -DIMENSIONAL BOOLEAN FUNCTIONS, $\forall n \geq 2$ AND $\forall 0 \leq p \leq \frac{1}{2}$

Lemma 1: For any $k \in \{1, 2, \dots, n\}$, let $\mathbf{Y} = [y_1 y_2 \dots y_k] \in \{0, 1\}^k$ be fixed and $\mathbf{X}^{(i)} = [x_1^{(i)} x_2^{(i)} \dots x_k^{(i)}] \in \{0, 1\}^k$ range over all the 2^k possible values. Then, the following identity holds $\sum_{i=1}^{2^k} p(\mathbf{Y}, \mathbf{X}^{(i)}) = \frac{1}{2^k}$.

Proof: $\mathbf{X}^{(i)}$ ranges from $[0 \ 0 \dots 0]$ to $[1 \ 1 \dots 1]$. For any fixed \mathbf{Y} , there is one $\mathbf{X}^{(i)}$, such that $\mathbf{X}^{(i)} = \mathbf{Y}$. There are $\binom{k}{1}$ number of vectors $\mathbf{X}^{(i)}$ that differ from \mathbf{Y} in one position. There are $\binom{k}{j}$ number of vectors $\mathbf{X}^{(i)}$ that differ from \mathbf{Y} in j positions. As a result, the summation of the joint probabilities becomes $\sum_{i=1}^{2^k} p(\mathbf{Y}, \mathbf{X}^{(i)}) = \sum_{i=1}^{2^k} \prod_{j=1}^k p(y_j, x_j^{(i)}) = \sum_{r=0}^k \binom{k}{r} \cdot \frac{(1-p)^{k-r} \cdot p^r}{2^k} = \frac{1}{2^k}$. ■

A. Boolean functions from the classes 1 and 2 of Theorem 1

In order to apply Karamata's inequality [2], we need to transform the mutual information into an algebraic expression. To this end, we employ concepts from probability mass functions of transformations of random variables [Ch 5, section 6 of [12]]. Let \mathbf{X}, \mathbf{Y} be two n -dimensional discrete random vectors, with ensembles $\mathcal{E}_X, \mathcal{E}_Y$, Z a discrete random variable, with ensemble \mathcal{E}_Z , and an n -dimensional function f , such that $Z = f(\mathbf{X})$. Let \mathbf{T}, \mathbf{U} be two random vectors and g be a multidimensional function, such that $\mathbf{T} = g_1(\mathbf{X}, \mathbf{Y}) = \mathbf{Y}$, $\mathbf{U} = g_2(\mathbf{X}, \mathbf{Y}) = \mathbf{X}$ and $Z = g_3(\mathbf{X}, \mathbf{Y}) = f(\mathbf{X})$.

$$p_{\mathbf{T}\mathbf{U}\mathbf{Z}}(\mathbf{t}, \mathbf{u}, z) = \sum_{\mathbf{x} \in \mathcal{E}_X, \mathbf{y} \in \mathcal{E}_Y, g_2(\mathbf{x}, \mathbf{y}) = \mathbf{u}} \sum_{g_1(\mathbf{x}, \mathbf{y}) = \mathbf{t}, g_3(\mathbf{x}, \mathbf{y}) = z} p_{\mathbf{X}\mathbf{Y}}(\mathbf{x}, \mathbf{y})$$

$$\begin{aligned} p_{\mathbf{Y}\mathbf{Z}}(\mathbf{y}, 1) &= \sum_{\mathbf{u} \in \mathcal{E}_U} p_{\mathbf{T}\mathbf{U}\mathbf{Z}}(\mathbf{t}, \mathbf{u}, 1) = \sum_{\mathbf{u} \in \mathcal{E}_U, 1=f(\mathbf{u})} p_{\mathbf{X}\mathbf{Y}}(\mathbf{u}, \mathbf{t}) = \\ &= \sum_{\mathbf{x} \in \mathcal{E}_X, 1=f(\mathbf{x})} p_{\mathbf{X}\mathbf{Y}}(\mathbf{x}, \mathbf{y}); p_{\mathbf{Y}\mathbf{Z}}(\mathbf{y}, 0) = p_{\mathbf{Y}}(\mathbf{y}) - p_{\mathbf{Y}\mathbf{Z}}(\mathbf{y}, 1). \end{aligned}$$

Let $N_0, N_1, \{\mathbf{x}_i^{(0)}\}$ and $\{\mathbf{x}_k^{(1)}\}$, such that $f(\mathbf{x}_i^{(0)}) = 0$ and $f(\mathbf{x}_k^{(1)}) = 1, \forall i \in \{1, 2, \dots, N_0\}, \forall k \in \{1, 2, \dots, N_1\}$. For the first class of functions, $N_1 = 1, N_0 = 2^n - 1$. Then, $p_{\mathbf{Y}\mathbf{Z}}(\mathbf{y}, 1) = p_{\mathbf{X}\mathbf{Y}}(\mathbf{x}_1^{(1)}, \mathbf{y}), p_{\mathbf{Y}\mathbf{Z}}(\mathbf{y}, 0) = \frac{1}{2^n} - p_{\mathbf{Y}\mathbf{Z}}(\mathbf{y}, 1), \forall \mathbf{y} \in \mathcal{E}_Y = \{0, 1\}^n$. For any $\mathbf{x}_1^{(1)} \in \{0, 1\}^n$, there exists: one vector, that is $m_0 = 1, \mathbf{y}_{i_0} \in \{0, 1\}^n$, such that $\mathbf{y}_{i_0} = \mathbf{x}_1^{(1)}$, a number $m_1 = \binom{n}{1}$ of the vectors (\mathbf{y}_{i_1}) , $\forall i_1 \in \{m_0 + 1, m_0 + 2, \dots, m_0 + m_1\}$, such that (\mathbf{y}_{i_1}) differ from $\mathbf{x}_1^{(1)}$ in one position and a number $m_k = \binom{n}{k}$ of the vectors (\mathbf{y}_{i_k}) , $\forall i_k \in \{(m_0 + \dots + m_{k-1}) + 1, (m_0 + \dots + m_{k-1}) + 2, \dots, (m_0 + \dots + m_{k-1}) + m_k\}$, such that (\mathbf{y}_{i_k}) differ from $\mathbf{x}_1^{(1)}$ in k positions, $\forall k \in \{0, 1, 2, \dots, n\}$.

$$p_{\mathbf{Y}\mathbf{Z}}(\mathbf{y}_{i_k}, 1) = \frac{(1-p)^{n-k} \cdot p^k}{2^n}, p_{\mathbf{Y}\mathbf{Z}}(\mathbf{y}_{i_k}, 0) = \frac{1}{2^n} -$$

$$p_{\mathbf{Y}\mathbf{Z}}(\mathbf{y}_{i_k}, 1), \forall i_k \in \{(m_0 + \dots + m_{k-1}) + 1, \dots,$$

$$(m_0 + \dots + m_{k-1}) + m_k\}, m_k = \binom{n}{k}, \forall k \in \{0, 1, \dots, n\}.$$

$$p_Z(1) = \sum_{i=1}^{2^n} p_{\mathbf{Y}\mathbf{Z}}(\mathbf{y}_i, 1) = \frac{1}{2^n}, p_Z(0) = 1 - p_Z(1) = \frac{2^n - 1}{2^n}.$$

$$\begin{aligned} \text{MI}(\mathbf{Y}, Z) &= \sum_{\mathbf{y}} \sum_z p_{\mathbf{Y}\mathbf{Z}}(\mathbf{y}, z) \cdot \log \frac{p_{\mathbf{Y}\mathbf{Z}}(\mathbf{y}, z)}{p_{\mathbf{Y}}(\mathbf{y}) \cdot p_Z(z)} \\ &= 2n + \sum_{\mathbf{y}} (2^n - 1) \cdot \frac{p_{\mathbf{Y}\mathbf{Z}}(\mathbf{y}, 0)}{2^n - 1} \cdot \log \frac{p_{\mathbf{Y}\mathbf{Z}}(\mathbf{y}, 0)}{2^n - 1} + \\ &\quad + p_{\mathbf{Y}\mathbf{Z}}(\mathbf{y}, 1) \cdot \log [p_{\mathbf{Y}\mathbf{Z}}(\mathbf{y}, 1)]. \end{aligned} \quad (1)$$

From this discussion, we can conclude that the mutual information is identical for all Boolean functions from the class of functions with $N_1 = 1$ and $N_0 = 2^n - 1$.

Let $\mathbf{q} = \{q_i\}$, $\mathbf{p} = \{p_i\}$ and $\mathbf{w} = \{w_i\}$, $\forall i \in \{1, 2, \dots, 2^n\}$, such that, $\forall k \in \{0, 1, \dots, n\}$,

$$q_i = p_{\mathbf{Y}\mathbf{Z}}(\mathbf{y}_{i_k}, 1) = \frac{(1-p)^{n-k} \cdot p^k}{2^n}, m_k = \binom{n}{k},$$

$$\forall i_k \in \{(\sum_{j=0}^{k-1} m_j + 1, \sum_{j=0}^{k-1} m_j + 2, \dots, \sum_{j=0}^{k-1} m_j + m_k\},$$

$$p_i = \frac{p_{\mathbf{Y}\mathbf{Z}}(\mathbf{y}_{i_k}, 0)}{2^n - 1} = \frac{1 - (1-p)^{n-k} \cdot p^k}{(2^n - 1) \cdot 2^n} = \frac{w_i}{2^n}.$$

$$\Rightarrow \text{MI}(\mathbf{Y}, Z) = 2n + \sum_{i=1}^{2^n} (2^n - 1) \cdot p_i \cdot \log p_i + \sum_{i=1}^{2^n} q_i \cdot \log q_i.$$

$$\begin{aligned} \sum_{i=1}^{2^n} q_i \cdot \log q_i &= \sum_{k=0}^n \binom{n}{k} \cdot \frac{(1-p)^{n-k} \cdot p^k}{2^n} \cdot \log \frac{(1-p)^{n-k} \cdot p^k}{2^n} \\ &= \frac{-n}{2^n} \cdot \sum_{k=0}^n \binom{n}{k} \cdot (1-p)^{n-k} \cdot p^k + \frac{\log(1-p)}{2^n} \cdot \sum_{k=0}^n (n-k) \cdot \binom{n}{k}. \end{aligned}$$

$$\begin{aligned}
& \cdot (1-p)^{n-k} \cdot p^k + \frac{\log p}{2^n} \cdot \sum_{k=1}^n k \cdot \binom{n}{k} \cdot (1-p)^{n-k} \cdot p^k \\
& (n-k) \cdot \binom{n}{k} = \frac{n \cdot (n-1)!}{k! \cdot (n-k-1)!} = n \cdot \binom{n-1}{k} \\
& k \cdot \binom{n}{k} = \frac{n \cdot (n-1)!}{(k-1)! \cdot (n-1-k+1)!} = n \cdot \binom{n-1}{k-1} \\
& \sum_{i=1}^{2^n} q_i \cdot \log q_i = \frac{-n}{2^n} + \frac{n \cdot (1-p) \cdot \log(1-p)}{2^n} \sum_{k=0}^{n-1} \binom{n-1}{k} \\
& \cdot (1-p)^{n-1-k} \cdot p^k + \frac{n \cdot p \cdot \log p}{2^n} \cdot \sum_{k=1}^n \binom{n-1}{k-1} \cdot p^{k-1} \\
& \cdot (1-p)^{n-1-k+1} = -\frac{n}{2^n} - \frac{n}{2^n} \cdot H(p) \\
& \sum_{i=1}^{2^n} (2^n-1) \cdot p_i \cdot \log p_i = \frac{2^n-1}{2^n} \cdot \left(-n + \sum_{i=1}^{2^n} w_i \cdot \log w_i \right)
\end{aligned}$$

Let $a = \frac{1-p}{2^{n-1}}$ and $b = \frac{p}{2^{n-1}}$. We want to prove that

$$\begin{aligned}
& \text{MI}(\mathbf{Y}, Z) \leq 1 - H(p) \Leftrightarrow \sum_{i=1}^{2^n} (2^n-1) \cdot w_i \cdot \log w_i \leq \\
& \leq (-n) \cdot (n-1) + (2^n-n) \cdot 2^{n-1} \cdot (a \cdot \log a + b \cdot \log b), \\
& \text{where } H(p) = -p \cdot \log p - (1-p) \cdot \log(1-p). \quad (2)
\end{aligned}$$

We need to transform the element $(-n) \cdot (n-1)$, from the right side of the inequality, into a sum of the type $x \cdot \log x$, such that the number of elements on the right side of the inequality equals that of the left side. That is, we need $2^n \cdot (2^n-1) - 2 \cdot 2^{n-1} \cdot (2^n-n) = (n-1) \cdot 2^n$ elements. That is, we need to find x , such that $(n-1) \cdot 2^n \cdot x \cdot \log x = (-n) \cdot (n-1) \Leftrightarrow x = \frac{1}{2^n}$. The right hand side sequence has three distinct elements ordered as $a = \frac{1-p}{2^{n-1}} \geq c = \frac{1}{2^n} \geq b = \frac{p}{2^{n-1}}$. The left hand side sequence has the elements ordered as $w_{2^n} = \frac{1-p^n}{2^{n-1}} \geq w_{2^n-1} = \frac{1-(1-p) \cdot p^{n-1}}{2^{n-1}} \geq \dots \geq w_i = \frac{1-(1-p)^{n-k} \cdot p^k}{2^{n-1}} \geq \dots \geq w_1 = \frac{1-(1-p)^n}{2^{n-1}}$. Let $\mathbf{X} = [x_1 \ x_2 \ \dots \ x_{2^n \cdot (2^n-1)}]$ and $\mathbf{Y} = [y_1 \ y_2 \ \dots \ y_{2^n \cdot (2^n-1)}]$ be equal to

$$\begin{aligned}
\mathbf{X} &= \begin{bmatrix} \underbrace{a \ a \ \dots \ a}_{2^{n-1} \cdot (2^n-n)} & \underbrace{c \ c \ \dots \ c}_{2^n \cdot (n-1)} & \underbrace{b \ b \ \dots \ b}_{2^{n-1} \cdot (2^n-n)} \\ \text{elements} & \text{elements} & \text{elements} \end{bmatrix}, \\
\mathbf{Y} &= \begin{bmatrix} \underbrace{w_{2^n}}_{2^{n-1}} & \underbrace{w_{2^n-1}}_{2^{n-1}} & \dots & \underbrace{w_1}_{2^{n-1}} \\ \text{elements} & \text{elements} & & \text{elements} \end{bmatrix}. \quad (3)
\end{aligned}$$

$\Rightarrow \mathbf{X}$ and \mathbf{Y} are in descending order, which satisfies the first condition of Karamata's theorem [2]. Let $g: \mathbb{R}_+ \rightarrow \mathbb{R}$, $g(x) = x \cdot \log x$. Then, g is a convex function.

1) We prove that $w_{2^n} \leq a$: $\Leftrightarrow \frac{1-p^n}{2^{n-1}} \leq \frac{1-p}{2^{n-1}} \Leftrightarrow (2^n-1) \cdot p - 2^{n-1} \cdot p^n \leq 2^{n-1} - 1$. Let $f(x): [0, \frac{1}{2}] \rightarrow \mathbb{R}_+$, $f(x) = (2^n-1) \cdot x - 2^{n-1} \cdot x^n$. $f'(x) = 2^n-1 - 2^{n-1} \cdot n \cdot x^{n-1} \geq n - 2^{n-1} \cdot n \cdot \frac{1}{2^{n-1}} = 0 \Rightarrow f'(x) \geq 0, \forall x \in [0, \frac{1}{2}]$, \Rightarrow the function f is increasing. Let x^* be the critical point of f . $f'(x) = 0 \Rightarrow (x^*)^{n-1} = \frac{2^n-1}{2^{n-1} \cdot n} \geq \frac{1}{2^{n-1}} \Rightarrow x^* \geq \frac{1}{2} \Rightarrow$

$f(x) \leq f(\frac{1}{2}), \forall x \in [0, \frac{1}{2}] \Rightarrow (2^n-1) \cdot p - 2^{n-1} \cdot p^n \leq 2^{n-1} - 1 \Rightarrow w_{2^n} \leq a$.

Let SL_k and SR_k , $\forall k \in \{1, 2, \dots, 2^n \cdot (2^n-1)\}$, denote the partial sums computed with the elements of the left-hand sequence of the inequality (2) and with the right-hand one, respectively. Let $K = 2^{n-1} \cdot (2^n-n)$. Using the binomial theorem [13], $2^{n-1} \geq 1 + n - 1 \Rightarrow 2^{n-1} \cdot \frac{(n-1)}{2^{n-1}-1} \leq 2^{n-1} \leq 2^n - 1 \Rightarrow 2^n - 1 \leq 2^{n-1} \cdot (2^n-n)$. $w_k \leq w_{2^n} \leq a, \forall k \in \{2^n, 2^n-1, \dots, 1\} \Rightarrow \text{SL}_k = \sum_{j=1}^k y_j \leq \text{SR}_k = \sum_{j=1}^k x_j = k \cdot x_1 = k \cdot a, \forall k \in \{1, 2, \dots, K\}$.

2) We prove that $2 \cdot w_{2^n} \leq a + c$: $\Leftrightarrow 2 \cdot \frac{1-p^n}{2^{n-1}} + \frac{p}{2^{n-1}} \leq \frac{3}{2^n}$. Let $f(x): [0, \frac{1}{2}] \rightarrow \mathbb{R}_+$, $f(x) = 2 \cdot \frac{1-x^n}{2^{n-1}} + \frac{x}{2^{n-1}}$. Using the binomial theorem [13], $\frac{2 \cdot n}{2^{n-1}} \leq 1 \Rightarrow \frac{2 \cdot n \cdot x^{n-1}}{2^{n-1}} \leq \frac{1}{2^{n-1}}, \forall 0 \leq x \leq \frac{1}{2}$. $f'(x) = \frac{-2 \cdot n \cdot x^{n-1}}{2^{n-1}} + \frac{1}{2^{n-1}} \Rightarrow f'(x) \geq 0, \forall 0 \leq x \leq \frac{1}{2} \Rightarrow f$ is increasing $\Rightarrow f(x) \leq f(\frac{1}{2}), \forall 0 \leq x \leq \frac{1}{2} \Rightarrow 2 \cdot \frac{1-p^n}{2^{n-1}} + \frac{p}{2^{n-1}} \leq \frac{3}{2^n} \Rightarrow 2 \cdot w_{2^n} \leq a + c$.

3) We prove that the inequalities involving the partial sums from Karamata's theorem hold: . If $n = 2$, it can be easily verified that $\text{SL}_{K+i} \leq 4 \cdot a + i \cdot c = \text{SR}_{K+i}, \forall i \in \{1, 2, 3, 4\}$. If $n \geq 3$, using the binomial theorem [13], we have that $K - 2^n \cdot (n-1) \geq 1, \forall n \geq 3$; $2 \cdot w_{2^n} \leq a + c \Rightarrow w_j + w_k \leq a + c, \forall j, k \in \{2^n, 2^n-1, \dots, 1\} \Leftrightarrow y_j + y_k \leq x_1 + x_{K+1}, \forall j, k \in \{2^n \cdot (2^n-1), 2^n \cdot (2^n-1) - 1, \dots, 1\}$; $K - i \geq 1, \forall i \in \{1, 2, \dots, 2^n \cdot (n-1)\} \Rightarrow \text{SL}_{K+i} = \text{SL}_{K-i} + y_{K-i+1} + \dots + y_K + y_{K+1} + \dots + y_{K+i} = \text{SL}_{K-i} + (y_{K-i+1} + y_{K+1}) + \dots + (y_K + y_{K+i}) \Rightarrow \text{SL}_{K+i} \leq \text{SR}_{K-i} + i \cdot (x_1 + x_{K+1}) = \text{SR}_{K+i}, \forall i \in \{1, 2, \dots, 2^n \cdot (n-1)\} \Rightarrow \text{SL}_{K+i} \leq \text{SR}_{K+i}, \forall i \in \{1, 2, \dots, 2^n \cdot (n-1)\}$.

4) We prove that $w_1 \geq b$: $\Leftrightarrow 2^{n-1} \geq 2^{n-1} \cdot (1-p)^n + (2^n-1) \cdot p$. Let $f(x): [0, \frac{1}{2}] \rightarrow \mathbb{R}_+$, $f(x) = 2^{n-1} \cdot (1-x)^n + (2^n-1) \cdot x$. Let x^* be the critical point of f . $f'(x) = 2^{n-1} \cdot n \cdot (1-x)^{n-1} \cdot (-1) + (2^n-1)$, $f''(x) = n \cdot (n-1) \cdot 2^{n-1} \cdot (1-x)^{n-2} \geq 0, \forall x \in [0, \frac{1}{2}] \Rightarrow f$ is a convex function and x^* is a minimum point $\Rightarrow f(x) \leq f(0) = f(\frac{1}{2}) = 2^{n-1}, \forall x \in [0, \frac{1}{2}] \Rightarrow 2^{n-1} \geq 2^{n-1} \cdot (1-p)^n + (2^n-1) \cdot p \Rightarrow w_1 \geq b$.

5) We verify that the final inequalities involving the partial sums from Karamata's theorem hold: $\text{SL}_{2^n \cdot (2^n-1)} = \sum_{i=1}^{2^n} (2^n-1) \cdot w_i = 2^n - 1$. $\text{SR}_{2^n \cdot (2^n-1)} = (n-1) \cdot 2^n \cdot \frac{1}{2^n} + (2^n-n) \cdot 2^{n-1} \cdot \frac{1-p}{2^{n-1}} + (2^n-n) \cdot 2^{n-1} \cdot \frac{p}{2^{n-1}} = 2^n - 1 \Rightarrow \text{SL}_{2^n \cdot (2^n-1)} = \text{SR}_{2^n \cdot (2^n-1)} \Leftrightarrow \text{SL}_{2^n \cdot (2^n-1)-k} + k \cdot w_1 = \text{SR}_{2^n \cdot (2^n-1)-k} + k \cdot b, \forall k \in \{1, 2, \dots, 2^n-1\} \Leftrightarrow \text{SL}_{2^n \cdot (2^n-1)-k} = \text{SR}_{2^n \cdot (2^n-1)-k} + k \cdot (b - w_1), \forall k \in \{1, 2, \dots, 2^n-1\} \Rightarrow \text{SL}_{2^n \cdot (2^n-1)-k} \leq \text{SR}_{2^n \cdot (2^n-1)-k}, \forall k \in \{1, 2, \dots, 2^n-1\}$.

In (II-A1), we proved that $2^n - 1 \leq 2^{n-1} \cdot (2^n - n)$. $K = 2^{n-1} \cdot (2^n - n)$ represents the total number of elements equal to b . The partial sum inequalities hold only for $2^n - 1$ elements equal to b . We need to determine that the remaining number of elements equal to b , satisfy the partial sum inequalities. We denote them as $\{\text{SL}_{2^n \cdot (2^n-1)-2^n, \dots, \text{SL}_{2^n \cdot (2^n-1)-2^{n-1} \cdot (2^n-n)+1}\}$ and $\{\text{SR}_{2^n \cdot (2^n-1)-2^n, \dots, \text{SR}_{2^n \cdot (2^n-1)-2^{n-1} \cdot (2^n-n)+1}\}$.

Let $M = 2^n \cdot (2^n-1) - (2^n-1)$. $\text{SL}_M = \sum_{j=1}^{M-i} y_j + y_{M-i+1} + \dots + y_M \leq \text{SR}_M = \sum_{j=1}^{M-i} x_j + x_{M-i+1} + \dots + x_M, \forall i \in \{1, 2, \dots, 2^{n-1} \cdot (2^n-n) - (2^n-1)\} \Rightarrow \text{SL}_{M-i} \leq$

$\text{SR}_{M-i} + (b - y_{M-i+1}) + \dots + (b - y_M) \leq \text{SR}_{M-i}, \forall i \in \{1, 2, \dots, 2^{n-1} \cdot (2^n - n) - (2^n - 1)\} \Rightarrow \text{SL}_{M-i} \leq \text{SR}_{M-i}, \forall i \in \{1, 2, \dots, 2^{n-1} \cdot (2^n - n) - (2^n - 1)\}$. These sums are well defined, because $M - i \geq 1, \forall i \in \{1, 2, \dots, 2^{n-1} \cdot (2^n - n) - (2^n - 1)\}$. $\forall i \in \{1, 2, \dots, 2^{n-1} \cdot (2^n - n) - (2^n - 1)\} \Rightarrow M - i \geq [2^n \cdot (2^n - 1) - (2^n - 1)] - [2^{n-1} \cdot (2^n - n) - (2^n - 1)] \Leftrightarrow M - i \geq 2^n \cdot (2^n - 1) - 2^{n-1} \cdot (2^n - n)$.

The first partial sum that does not contain an element equal to b is given by $i = 2^{n-1} \cdot (2^n - n) - (2^n - 1) \Rightarrow M - i = 2^n \cdot (2^n - 1) - 2^{n-1} \cdot (2^n - n) = K + 2^n \cdot (n - 1)$. As a result, $\text{SL}_{K+2^n \cdot (n-1)} \leq \text{SR}_{K+2^n \cdot (n-1)}$, which we also proved in (II-A3). In conclusion, all the conditions in Karamata's theorem are satisfied. This yields $\sum_{i=1}^{2^{n-1} \cdot (2^n - 1)} g(y_i) \leq \sum_{i=1}^{2^n \cdot (2^n - 1)} g(x_i) \Leftrightarrow \text{MI}(\mathbf{Y}, Z) \leq 1 - H(p)$.

Following the above reasoning, the same result holds, for Boolean functions that have one element equal to 0 in their output table and the rest are equal to 1, that is $N_1 = 2^n - 1$ and $N_0 = 1$.

B. Boolean functions from the classes 3 and 4 of Theorem 1

For any $r \in \{1, 2, \dots, n - 1\}$, let $N_1 = 2^{n-r}$ and $\mathbf{Y}^{(k)} = [\mathbf{Y}_r^{(k)} \mathbf{Y}_{n-r}^{(k)}], \forall k \in \{1, 2, \dots, 2^n\}$, and $\mathbf{X}^{(i)} = [\mathbf{X}_r \mathbf{X}_{n-r}^{(i)}], \forall i \in \{1, 2, \dots, 2^{n-r}\}$, such that $\mathbf{X}^{(i)} \in \{[\mathbf{X}_r \ 0 \ 0 \dots 0 \ 0], [\mathbf{X}_r \ 0 \ 0 \dots 0 \ 1], \dots, [\mathbf{X}_r \ 1 \ 1 \dots 1 \ 1]\}$. The output table of the Boolean function has $N_1 = 2^{n-r}$ number of ones, such that these values correspond to the vector of inputs $\mathbf{X}^{(i)} \in \{[\mathbf{X}_r \ 0 \ 0 \dots 0 \ 0], [\mathbf{X}_r \ 0 \ 0 \dots 0 \ 1], \dots, [\mathbf{X}_r \ 1 \ 1 \dots 1 \ 1]\}$, where \mathbf{X}_r is fixed. The rest of the output values are zeros.

From the properties of the binary symmetric channel, we have that $p(\mathbf{Y}^{(k)}, \mathbf{X}^{(i)}) = p(\mathbf{Y}_r^{(k)}, \mathbf{X}_r) \cdot p(\mathbf{Y}_{n-r}^{(k)}, \mathbf{X}_{n-r}^{(i)}), \forall k \in \{1, 2, \dots, 2^n\}$. According to Lemma 1, $\sum_{i=1}^{2^{n-r}} p(\mathbf{Y}_{n-r}^{(k)}, \mathbf{X}_{n-r}^{(i)}) = \frac{1}{2^{n-r}}$. Let $q_k = p_{\mathbf{Y}Z}(\mathbf{Y}^{(k)}, 1) = \sum_{i=1}^{2^{n-r}} p(\mathbf{Y}^{(k)}, \mathbf{X}^{(i)}) = \sum_{i=1}^{2^{n-r}} p(\mathbf{Y}_r^{(k)}, \mathbf{X}_r) \cdot p(\mathbf{Y}_{n-r}^{(k)}, \mathbf{X}_{n-r}^{(i)}) = \frac{p(\mathbf{Y}_r^{(k)}, \mathbf{X}_r)}{2^{n-r}}$. Let $p_k = p_{\mathbf{Y}Z}(\mathbf{Y}^{(k)}, 0) = p_{\mathbf{Y}}(\mathbf{Y}^{(k)}) - p_{\mathbf{Y}Z}(\mathbf{Y}^{(k)}, 1) = \frac{1}{2^n} - p_{\mathbf{Y}Z}(\mathbf{Y}^{(k)}, 1), \forall k \in \{1, 2, \dots, 2^n\}$. For any $k \in \{1, 2, \dots, 2^n\}$, the total number of $\mathbf{Y}^{(k)} = [\mathbf{Y}_r^{(k)} \mathbf{Y}_{n-r}^{(k)}]$ that have the same $\mathbf{Y}_r^{(k)}$ is equal to $N_1 = 2^{n-r}$. This produces a number of $N_1 = 2^{n-r}$ identical probability mass values, $q_k = \frac{p(\mathbf{Y}_r^{(k)}, \mathbf{X}_r)}{2^{n-r}}$ and $N_1 = 2^{n-r}$ identical probability mass values, $p_k = \frac{1}{2^n} - q_k$. Let the vectors $\mathbf{v} = [v_1 \ v_2 \dots v_{2^r}]$ and $\mathbf{t} = [t_1 \ t_2 \dots t_{2^r}]$ denote the distinct values of the vectors $\mathbf{q} = [q_1 \ q_2 \dots q_{2^n}]$ and $\mathbf{p} = [p_1 \ p_2 \dots p_{2^n}]$, respectively.

$$\text{MI}(\mathbf{Y}, Z) = 2n + 2^{n-r} \sum_{i=1}^{2^r} t_i \cdot \log \frac{t_i}{2^n - 2^{n-r}} + v_i \cdot \log \frac{v_i}{2^{n-r}}$$

For any $\mathbf{X}_r \in \{0, 1\}^r$ fixed, there exists: one vector, that is $m_0 = 1, \mathbf{Y}_r^{(i_0)} \in \{0, 1\}^r$, such that $\mathbf{Y}_r^{(i_0)} = \mathbf{X}_r$, a number $m_1 = \binom{r}{1}$ of the vectors $(\mathbf{Y}_r^{(i_1)})$, $\forall i_1 \in \{m_0 + 1, m_0 + 2, \dots, m_0 + m_1\}$, such that $(\mathbf{Y}_r^{(i_1)})$ differ from \mathbf{X}_r in one position and a number $m_j = \binom{r}{j}$ of the vectors $(\mathbf{Y}_r^{(i_j)})$,

$\forall i_j \in \{(m_0 + \dots + m_{j-1}) + 1, (m_0 + \dots + m_{j-1}) + 2, \dots, (m_0 + \dots + m_{j-1}) + m_j\}$, such that $(\mathbf{Y}_r^{(i_j)})$ differ from \mathbf{X}_r in j positions, $\forall j \in \{0, 1, 2, \dots, r\}$. As a result, we obtain

$$\begin{aligned} p(\mathbf{Y}_r^{(i_j)}, \mathbf{X}_r) &= \frac{(1-p)^{r-j} \cdot p^j}{2^r}, m_j = \binom{r}{j}, \forall j \in \{0, 1, \dots, r\} \\ \forall i_j \in \{(m_0 + \dots + m_{j-1}) + 1, \dots, (m_0 + \dots + m_{j-1}) + m_j\} \\ v_i &= \frac{(1-p)^{r-j} \cdot p^j}{2^r \cdot 2^{n-r}}, t_i = \frac{1 - (1-p)^{r-j} \cdot p^j}{2^n} \\ \Rightarrow \text{MI}(\mathbf{Y}, Z) &= 2r + \sum_{i=1}^{2^r} (2^{n-r} \cdot t_i) \cdot \log \frac{(2^{n-r} \cdot t_i)}{2^r - 1} + \\ &+ (2^{n-r} \cdot v_i) \cdot \log (2^{n-r} \cdot v_i) \leq 1 - H(p). \end{aligned} \quad (4)$$

The last inequality represents the result proved for Boolean functions from the classes 1 and 2, with $n = r$. Equality is obtained for $r = 1$, that is for the dictatorship function. If $r = 1 \Rightarrow N_1 = 2^{n-1}, N_0 = 2^{n-1}, \mathbf{v} = [\frac{1-p}{2^n} \ \frac{p}{2^n}]$ and $\mathbf{t} = [\frac{p}{2^n} \ \frac{1-p}{2^n}] \Rightarrow \text{MI}(\mathbf{Y}, Z) = 1 - H(p)$.

Following the above reasoning, the same result holds, for Boolean functions that have $N_0 = 2^{n-r}$ elements equal to 0 in their output table and the rest are equal to 1, that is $N_1 = 2^n - 2^{n-r} = 2^{n-r} \cdot (2^r - 1), \forall r \in \{1, 2, \dots, n - 1\}$. These Boolean functions satisfy an additional condition: the 0 values from the output table correspond to the input vectors $\mathbf{X}^{(i)} = [\mathbf{X}_r \mathbf{X}_{n-r}^{(i)}] \in \{[\mathbf{X}_r \ 0 \ 0 \dots 0 \ 0], [\mathbf{X}_r \ 0 \ 0 \dots 0 \ 1], \dots, [\mathbf{X}_r \ 1 \ 1 \dots 1 \ 1]\}$, where \mathbf{X}_r is fixed, $\forall i \in \{1, 2, \dots, 2^{n-r}\}$.

III. CONCLUSIONS

In this study, we proved the Courtade-Kumar conjecture, for certain subclasses of Boolean lex functions, for all dimensions, $\forall n \geq 2$, and for all values of the error probability, $\forall 0 \leq p \leq \frac{1}{2}$. We provided an algebraic proof using Karamata's theorem as our main tool. We brought further improvement in the effort to establish this conjecture in its most general form. Our novelty lied in showing that, for several subclasses of Boolean lex functions, the conjecture holds for all dimensions, $\forall n \geq 2$, and for all values of the error probability, $\forall 0 \leq p \leq \frac{1}{2}$. We have tried to apply Karamata's theorem to other types of Boolean functions, in order to solve the conjecture in its most general form. However, we have been unsuccessful in both applying the theorem directly to the mutual information inequality and in finding a suitable algebraic transformation of the original inequality into an expression that can be proved with Karamata's theorem. The majorization condition from this theorem cannot be verified.

IV. ACKNOWLEDGMENTS

We would like to thank Thomas Courtade for helpful discussions on lex functions and for indicating two articles which employ Karamata's theorem and its extension, Schur convexity, namely an earlier version of the preprint [4] and [3], respectively.

REFERENCES

- [1] T. A. Courtade and G. R. Kumar, "Which Boolean functions maximize mutual information on noisy inputs?" *IEEE Transactions on Information Theory*, vol. 60, no. 8, pp. 4515–4525, August 2014.
- [2] J. Karamata, "Sur une inégalité relative aux fonctions convexes," *Publications de l'Institut Mathématique*, vol. 1, no. 1, pp. 145–147, 1932.
- [3] G. R. Kumar and T. A. Courtade, "Which Boolean functions are most informative?" in *Proceedings of the 2013 IEEE International Symposium on Information Theory (ISIT 2013)*, 2013.
- [4] G. Kindler, R. O'Donnell, and D. Witmer, "Continuous analogues of the most informative function problem," preprint, arXiv:1506.03167v3.
- [5] O. Ordentlich, O. Shayevitz, and O. Weinstein, "An improved upper bound for the most informative Boolean function conjecture," in *Proceedings of the 2016 International Symposium on Information Theory (ISIT 2016)*, 2016.
- [6] A. Samorodnitsky, "On the entropy of a noisy function," *IEEE Transactions on Information Theory*, vol. 62, no. 10, pp. 5446–5464, October 2016.
- [7] E. Erkip, "The efficiency of information in investment," Doctor of Philosophy dissertation, Stanford University, Department of Electrical Engineering, August 1996.
- [8] A. D. Wyner and J. Ziv, "A theorem on the entropy of certain binary sequences and applications: part I," *IEEE Transactions on Information Theory*, vol. IT-19, no. 6, pp. 769–772, November 1973.
- [9] V. Anantharam, A. A. Gohari, S. Kamath, and C. Nair, "On hypercontractivity and the mutual information between Boolean functions," in *Proceedings of the 2013 51st Annual Allerton Conference on Communication, Control and Computing*, 2013.
- [10] F. P. Calmon, M. Varia, and M. Médard, "An exploration of the role of principal inertia components in information theory," in *Proceedings of the 2014 IEEE Information Theory Workshop (ITW 2014)*, 2014.
- [11] G. Pichler, G. Matz, and P. Piantanida, "A tight upper bound on the mutual information of two Boolean functions," in *Proceedings of the 2016 IEEE Information Theory Workshop (ITW 2016)*, 2016.
- [12] A. M. Mood, F. A. Graybill, and D. C. Boes, *Introduction to the theory of statistics*, 3rd ed. McGraw-Hill, 1974.
- [13] M. Abramovitz and I. A. Stegun, Eds., *Handbook of mathematical functions with formulas, graphs and mathematical tables*. Tenth Printing, December 1972.